

# Department of Commerce



## Information Technology Security Compliance Review Metrics

As recommended by the Working Group on  
Compliance Review Metrics

**(Revision 1, May 1, 2002)**

## ***Table of Contents***

<b><i>Executive Summary</i></b>	<b><i>ii</i></b>
<b><i>1. PURPOSE</i></b>	<b><i>1</i></b>
<b><i>2. BACKGROUND</i></b>	<b><i>1</i></b>
<b><i>3. COMPLIANCE AND ENFORCEMENT</i></b>	<b><i>2</i></b>
<b><i>3.1 Compliance Review Framework</i></b>	<b><i>3</i></b>
<b><i>3.2 Program Requirements</i></b>	<b><i>5</i></b>
<b><i>3.3 System Requirements</i></b>	<b><i>15</i></b>
<b><i>4. WAIVERS</i></b>	<b><i>16</i></b>
<b><i>5. APPENDICES</i></b>	<b><i>17</i></b>
<b><i>Appendix I - Acronyms</i></b>	<b><i>18</i></b>
<b><i>Appendix II - Applicable Laws, Regulations and Policy</i></b>	<b><i>19</i></b>
<b><i>Appendix III - Working Group Members</i></b>	<b><i>20</i></b>
<b><i>Appendix IV - Modified FISCAM</i></b>	<b><i>21</i></b>

## ***Executive Summary***

**The Department of Commerce established a working group to develop the criteria used to evaluate compliance of operating unit information technology (IT) security programs. Additionally, the working group has established metrics for reviewing compliance of system level information technology security documentation with the program requirements of the Department's information technology security program.**

**The purpose of this document is to:**

- **Ensure that Department and operating unit level information technology security programs and policies are consistent with each other;**
- **Set forth the Department of Commerce Information Technology Security Compliance Metrics to ensure consistency in review technique and terminology;**
- **Provide metrics for validation of an operating unit's implementation of its information technology security programs and policies through the use of a baseline methodology to evaluate information technology security programs;**
- **Provide information for compliance reviewers and identify the compliance metrics that will be used to evaluate operating unit IT security programs; and**
- **Provide a framework that makes effective use of information, best practices, and lessons learned that are identified during compliance reviews to enhance Department and operating unit programs and policies.**

**The conceptual framework for the development of the recommended metrics for program review, are the list of elements for Department IT security programs, as described in the Department of Commerce IT Security Task Force, Working Group on Department-wide Information Technology Security Program recommendations (Recommended ITS Program Structure). The metrics used for system compliance evaluation are at Appendix IV of this document as discussed in the *Financial Information System Controls Audit Manual* (FISCAM).**

# Department of Commerce

## Information Technology Security Compliance Review Metrics

*(Revision 1, May 1, 2002)*

### **1. PURPOSE**

The purpose of this document is to set forth the Department of Commerce Information Technology (IT) Security Compliance Metrics and to ensure consistency in review techniques and terminology. Specifically, this document will:

- Ensure that Department and operating unit-level information technology security programs and policies are consistent with each other;
- Provide metrics for validation of an operating unit's implementation of its IT security programs and policies through the use of a baseline methodology to evaluate information technology security programs; and
- Provide a framework that makes effective use of information, best practices, and lessons learned that are identified during compliance reviews to enhance Department and operating unit programs and policies.

### **2. BACKGROUND**

There has been an increasing reliance on information technology resources to accomplish the complex mission of the Department of Commerce and its operating units. This has included the rise in the number and types of computer systems used, their interconnection through telecommunication networks and the increasingly complex standards and policies governing these IT security resources. At the same time that the Department has seen this increase in reliance on new technologies, there has been a corresponding increase in the threat to the Department's resources and data.

The Department of Commerce IT Security Program is the key element that provides the framework on which the Department and its operating units can build effective control measures to safeguard its sensitive and vital information resources and data.

Recent audits of the Department of Commerce IT Security Program highlighted the need to review and update the program. As a result, a working group on Department-wide Information Security Program was established to study the current IT Security Program and recommend an updated policy reflecting a new emphasis on how IT security is conducted within the Department of Commerce. The result of the Security Program Working Group was a document entitled "Recommended Information Security (ITS) Program Structure,"

issued on September 28, 2001. In October of 2001, a second working group was formed and using this document as a reference, developed a set of review metrics to indicate the degree to which security goals are being met. This document, which formalizes the review process and provides a consistent set of guidelines to be used throughout the Department of Commerce, is the result of that working group.

### **3. COMPLIANCE AND ENFORCEMENT**

The compliance review program will assess operating unit IT security programs and provide positive feedback to operating units on tasks being done well and identify best practices currently in place. These practices will be shared with all operating units.

In addition, a compliance review program will identify deficiencies associated with the operating unit IT security program that need to be improved, provide potential corrective actions, and track implementation of corrective actions. The IT Security Program elements to be assessed will include, at a minimum:

- Appointment of Operating Unit IT Security Officer.
- Development/maintenance of inventory of all IT systems.
- Development/updating of security plans for all IT systems.
- Performance of risk/vulnerability assessments for all IT systems.
- Security during the systems development life cycle.
- Development/updating of contingency plans for all IT systems and data centers and performance of annual testing of contingency plans.
- Development/maintenance of a Computer Security Awareness, Training, and Education Program for operating unit employees and contractor employees.
- Development of Computer Emergency Incident Response Team capabilities, including reporting of computer incidents & intrusions to the Department.
- Certification/accreditation for all IT systems.

The Office of the Inspector General provides independent oversight through audit and evaluation of the Department's IT Security Program in accordance with the "Inspector General's Act of 1978." For policies relating to these areas, refer to the appropriate Departmental directives (i.e., DAO 207-10).

### **3.1 Compliance Review Framework**

#### **3.1.1 Departmental Review of Operating Unit IT Security Programs**

##### **A. Measure against the Department's IT Security Program**

- Interviews of operating unit's Chief Information Officer (CIO) and Information Technology Security Officer (ITSO)
- Interviews of a sample of program managers and systems administrators
- In-depth review of several sample systems within an operating unit, including:
  - Review of risk assessments, system security and contingency plans, certification/accreditation process, and training program, and
  - Penetration testing.

##### **B. Review Cycle**

The review cycle should be consistent with Departmental policy for IT Security Program compliance reviews, for example, tri-annual reviews.

##### **C. Scope of coverage**

- All DOC operating units
- IT Security Program management procedures and controls
- Business continuity planning
- Operational compliance assessment, including:
  - System-specific policies,
  - Security assessments,
  - Security plans,
  - System certification and accreditation documentation,
  - System access controls,

- Computer incident reporting procedures,
- System-specific training, and
- Penetration testing.

### 3.1.2 Operating Unit Review

#### A. Evaluate operating unit IT Security Program

- Interviews of program managers and systems administrators
- In-depth review of each system to include:
  - Quality review of risk assessments, security and contingency plans, certification/accreditation process, and training
  - Penetration testing

#### B. Review Cycle

The review cycle should be consistent with operating unit policy for Information Technology Security Program compliance reviews.

#### C. Appropriate number of reviews each year to cover all operating unit IT systems over a three-year period.

- Review management procedures and controls
- Review business continuity planning
- Perform operational compliance assessment, including:
  - System-specific policies,
  - Security assessments,
  - Security plans,
  - System certification and accreditation documentation,
  - System access controls,

- Computer incident reporting procedures,
- System-specific training, and
- Penetration testing.

## 3.2 Program Requirements

Compliance reviews occur at several levels – the Department level, the operating unit or line office level. Comprehensive, high level reviews should be balanced with narrower, more in-depth reviews performed by operating units and line offices of programs and systems. A compliance-based approach assesses how closely established security standards are being followed. The framework used to derive these standards was the *Report of the Working Group on Department-wide Information Technology Security Program, Recommended ITS Program Structure, September 28, 2001*. A top-down approach was used to generate the specific method. It started with the objectives of the security program and then worked back to identify specific metrics that would help determine if those objectives are being met. Lastly a method to measure these techniques was needed to generate those metrics.

The Federal Information System Controls Audit Manual (FISCAM) contains six areas of controls, one of which addresses entity-wide security program planning and management. This area consists of controls that are meant to assess program-level compliance. Using the FISCAM metrics, the following table lists areas for measurement of program compliance. It is recommended that it need not be repeated in the system-level review.

### 3.2.1 Program-Level Program Management Metrics:

<b>Security Program Planning &amp; Management Compliance Area</b>		<b>Compliance Review Technique</b>	<b>Compliance Metric to Ensure Consistency with DOC program</b>
1	Appointment of operating unit IT Security Officer	Review appointment letter	Letter exists and is signed
2	Development/maintenance of inventory of all IT systems	Review System Inventory data  Validate accuracy of System Inventory data for major applications and general support systems selected for in-depth review	Inventory exists and is updated quarterly  System Inventory data is accurate
3	Development/updating of security plans for all IT systems	Review System Inventory data  Validate accuracy of System Inventory data for major applications and general support systems selected for in-depth review	Security plan for each system exists and is reviewed annually  System Inventory data is accurate
4	Performance of risk/vulnerability assessments for all IT systems	Review System Inventory data  Validate accuracy of System Inventory data for major applications and general support systems selected for in-depth review	Risk assessment for each system exists and is reviewed annually and updated at least every 3 years  System Inventory data is accurate
5	Security during the systems development life cycle	Review life cycle/development policy	Life cycle/development policy for each system exists and is reviewed annually and updated at least every 3 years.

Security Program Planning & Management Compliance Area		Compliance Review Technique	Compliance Metric to Ensure Consistency with DOC program
6	Development/updating of contingency plans for all IT systems and data centers.	Review System Inventory data  Validate accuracy of System Inventory data for major applications and general support systems selected for in-depth review	Contingency plan for each system exists and is reviewed annually and updated at least every 3 years  System Inventory data is accurate
7	Performance of annual testing of contingency plans	Interview operating unit CIO and ITSO, and SA  Review contingency plan policy	Annual testing of contingency plans are performed
8	Development/maintenance of a computer security awareness, training, and education program for operating unit and contractor employees	Review training plan  Review training records  Interview staff  Review personnel hiring, transfer and firing procedures	Entry-on-duty training is performed  Annual IT awareness training is given to all employees  Specialized IT Security training plans exist and are executed for those employees in sensitive security positions  Background checks of all employees are accomplished  Procedures for hiring, transfer, and firing of employees address IT security issues
9	Configuration Management Plan for Security Program	Review plan  Review policy management system	There are defined procedures for changes to the IT security program, and they are being followed

Security Program Planning & Management Compliance Area		Compliance Review Technique	Compliance Metric to Ensure Consistency with DOC program
10	Development of Computer Emergency Incident Response Team (CERT) or capability	<p>Review incident response capability or CERT documentation</p> <p>Review incident response reporting policy</p> <p>Interview CIO, ITSO, SA, NA, and employees</p> <p>Review MOAs, and customer agreements</p> <p>Review incident reports</p>	<p>Documentation exists that outlines CERT/incident response capabilities and responsibilities.</p> <p>Responders know what to do and who to notify in case of a suspected incident.</p> <p>Employees know what to do in the case of a suspected incident.</p> <p>Appropriate Incident Reports are forwarded to DOC.</p> <p>Can ascertain the % of attempted break-ins to successful intrusions</p>
11	Certification/accreditation for all systems	<p>Review System Inventory data</p> <p>Validate accuracy of System Inventory data for major applications and general support systems selected for in-depth review</p>	<p>Certification/accreditation documents for all systems exist and is reviewed annually and redone at least every 3 years</p> <p>System Inventory data is accurate</p>
12	Compliance Reviews Plan	<p>Review plan documentation</p> <p>Review completed reviews</p>	<p>Plans meet the criteria set forth in the DOC <i>Recommended ITS Program Structure</i>, 09/28/2001.</p> <p>Appropriate reviews, in accordance with the above reference, are being completed.</p>

### 3.2.2 Recommended Program-Level Policy Metrics:

<b>Security Policy Compliance Area</b>		<b>Individual Policy Compliance Review Technique</b>	<b>Compliance Metric to Ensure Policy exists and is reviewed annually</b>
1	Appropriate Use or Acceptable Use Policy	<p>Review policy</p> <p>Interview various levels of staff</p> <p>Verify audits are performed in accordance with the policy or tools are in place to enforce requirements</p>	<p>Policy exists</p> <p>Audits are performed as required or verify existence of tools</p>
2	Password Policy	<p>Review policy</p> <p>Interview various levels of staff</p> <p>Verify audits are performed in accordance with the policy or tools are in place to enforce requirements</p>	<p>Policy exists</p> <p>Audits are performed as required or verify existence of tools</p>
3	Information Sensitivity Policy	<p>Review policy</p> <p>Interview various levels of staff</p> <p>Verify audits are performed in accordance with the policy or tools are in place to enforce requirements</p>	<p>Policy exists</p> <p>Audits are performed as required or verify existence of tools</p>

Security Policy Compliance Area		Individual Policy Compliance Review Technique	Compliance Metric to Ensure Policy exists and is reviewed annually
4	Remote Access Policy	<p>Review policy</p> <p>Interview various levels of staff</p> <p>Verify audits are performed in accordance with the policy or tools are in place to enforce requirements</p>	<p>Policy exists</p> <p>Audits are performed as required or verify existence of tools</p>
5	Virus Protection and Prevention Policy	<p>Review policy</p> <p>Interview various levels of staff</p> <p>Verify audits are performed in accordance with the policy or tools are in place to enforce requirements</p>	<p>Policy exists</p> <p>Audits are performed as required or verify existence of tools</p>
6	Perimeter Security Policy	<p>Review policy</p> <p>Interview various levels of staff</p> <p>Verify audits are performed in accordance with the policy or tools are in place to enforce requirements</p>	<p>Policy exists</p> <p>Audits are performed as required or verify existence of tools</p>

Security Policy Compliance Area		Individual Policy Compliance Review Technique	Compliance Metric to Ensure Policy exists and is reviewed annually
7	Server/host Security Policy	<p>Review policy</p> <p>Interview various levels of staff</p> <p>Verify audits are performed in accordance with the policy or tools are in place to enforce requirements</p>	<p>Policy exists</p> <p>Audits are performed as required or verify existence of tools</p>
8	Router/switch Security Policy	<p>Review policy</p> <p>Interview various levels of staff</p> <p>Verify audits are performed in accordance with the policy or tools are in place to enforce requirements</p>	<p>Policy exists</p> <p>Audits are performed as required or verify existence of tools</p>
9	Wireless Access Policy	<p>Review policy</p> <p>Interview various levels of staff</p> <p>Verify audits are performed in accordance with the policy or tools are in place to enforce requirements</p>	<p>Policy exists</p> <p>Audits are performed as required or verify existence of tools</p>

<b>Security Policy Compliance Area</b>		<b>Individual Policy Compliance Review Technique</b>	<b>Compliance Metric to Ensure Policy exists and is reviewed annually</b>
10	Extranet Policy	<p>Review policy</p> <p>Interview various levels of staff</p> <p>Verify audits are performed in accordance with the policy or tools are in place to enforce requirements</p>	<p>Policy exists</p> <p>Audits are performed as required or verify existence of tools</p>
11	Segregation of duties/responsibility policy (system-level)	<p>Review policy</p> <p>Interview various levels of staff</p> <p>Verify audits are performed in accordance with the policy or tools are in place to enforce requirements</p>	<p>Policy exists</p> <p>Audits are performed as required or verify existence of tools</p>
12	Policy for distribution of responsibilities/functions among organization (organization-level)	<p>Review policy</p> <p>Interview various levels of staff</p> <p>Verify audits are performed in accordance with the policy or tools are in place to enforce requirements</p>	<p>Policy exists</p> <p>Audits are performed as required or verify existence of tools</p>

Security Policy Compliance Area		Individual Policy Compliance Review Technique	Compliance Metric to Ensure Policy exists and is reviewed annually
13	Network Security Policy	<p>Review policy</p> <p>Interview various levels of staff</p> <p>Verify audits are performed in accordance with the policy or tools are in place to enforce requirements</p>	<p>Policy exists</p> <p>Audits are performed as required or verify existence of tools</p>
14	Electronic commerce	<p>Review policy</p> <p>Interview various levels of staff</p> <p>Verify audits are performed in accordance with the policy or tools are in place to enforce requirements</p>	<p>Policy exists</p> <p>Audits are performed as required or verify existence of tools</p>
15	PKI	<p>Review policy</p> <p>Interview various levels of staff</p> <p>Verify audits are performed in accordance with the policy or tools are in place to enforce requirements</p>	<p>Policy exists</p> <p>Audits are performed as required or verify existence of tools</p>

<b>Security Policy Compliance Area</b>		<b>Individual Policy Compliance Review Technique</b>	<b>Compliance Metric to Ensure Policy exists and is reviewed annually</b>
16	Encryption Policy	Review policy Interview various levels of staff Verify audits are performed in accordance with the policy or tools are in place to enforce requirements	Policy exists Audits are performed as required or verify existence of tools
17	Internet & Firewall Security	Review policy Interview various levels of staff Verify audits are performed in accordance with the policy or tools are in place to enforce requirements	Policy exists Audits are performed as required or verify existence of tools
18	Intrusion Detection Monitoring	Review policy Interview various levels of staff Verify audits are performed in accordance with the policy or tools are in place to enforce requirements	Policy exists Audits are performed as required or verify existence of tools
19	Web Site Security	Review policy Interview various levels of staff Verify audits are performed in accordance with the policy or tools are in place to enforce requirements	Policy exists Audits are performed as required or verify existence of tools

[Note: In the event that time does not allow review of all program-level policy metrics, a representative portion of the policies will be made on an impartial basis. The recommended criteria for selecting security policies to review are

- Date of last policy review and nature of audit/review findings -- priority will be placed on those policies that received significant findings or were not reviewed, and
- Policies significant to the operation of critical infrastructure, business-essential, or mission critical systems.]

### 3.3 System-Level Compliance Review Requirements

For the much narrower system compliance review, it was noted that both GAO and OIG were using the FISCAM as their compliance metric. To maintain consistency, it was decided to recommend that a modified version of the FISCAM be used. The remaining five (5) areas of control in FISCAM are:

- **Access controls** that limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure;
- **Application software development and change controls** that prevent unauthorized programs or modifications to an existing program from being implemented;
- **System software controls** that limit and monitor access to the powerful programs and sensitive files that (1) control the computer hardware and (2) secure applications supported by the system;
- **Segregation of duties** that are policies, procedures, and an organizational structure established so that one individual cannot control key aspects of computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to assets or records; and
- **Service continuity controls** to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.

The modified FISCAM used for operating unit compliance reviews is located at Appendix IV.

#### **4. WAIVERS**

Operating units may request a waiver to criteria stated in this document. Waivers shall be sent to the Department of Commerce CIO for review. Waiver requests must include the following information:

- A. Specific criteria for which the waiver is requested;
- B. The reason the waiver is required;
- C. Description of the specific business case served by granting the waiver; and
- D. Alternative mitigating controls that address vulnerabilities that may be introduced by approving the waiver request.

## **APPENDICES**

## Appendix I

### Acronyms

<b>Acronyms</b>	<b>Replaces</b>
<b>CERT</b>	<b>Computer Emergency Response Team</b>
<b>CIO</b>	<b>Chief Information Officer</b>
<b>CIP</b>	<b>Critical Information Protection</b>
<b>DOC</b>	<b>Department of Commerce</b>
<b>FISCAM</b>	<b>Financial Information System Controls Audit Manual</b>
<b>GAO</b>	<b>General Accounting Office</b>
<b>GISRA</b>	<b>Government Information Security Reform Act</b>
<b>GPEA</b>	<b>Government Paperwork Elimination Act</b>
<b>IT</b>	<b>Information Technology</b>
<b>ITS</b>	<b>Information Technology Security</b>
<b>ITSO</b>	<b>IT Security Officer</b>
<b>MOA</b>	<b>Memorandum of Agreement</b>
<b>NA</b>	<b>Network Administrator</b>
<b>OIG</b>	<b>Office of the Inspector General</b>
<b>OMB</b>	<b>Office of Management and Budget</b>
<b>OU</b>	<b>Operating Unit</b>
<b>PKI</b>	<b>Public Key Infrastructure</b>
<b>SA</b>	<b>System Administrator</b>
<b>SO</b>	<b>Security Officer</b>

## Appendix II

### Applicable Laws, Regulations, Policies and References

1. Computer Security Act of 1987 (PL 100-235)
2. Government Information Security Reform Act (GISRA) (PL 106-398)
3. Guidance on Implementing GISRA (OMB 01-08)
4. OMB Circular A-123, *Management Accountability and Control*
5. OMB Circular A-127, *Financial Management Systems*
6. OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*
7. General Accounting Office's *Financial Information System Controls Audit Manual* (FISCAM)
8. Department of Commerce Information Technology Security Program Policy
9. Government Paperwork Elimination Act (GPEA) (PL 105-277, Title XVII, 44 USC 3504)
10. OMB Procedures and Guidelines for Implementing GPEA (OMB M-00-10)
11. IT Management Reform Act of 1996 - Clinger/Cohen Act (40 USC 1542)
12. Privacy Act of 1974 (PL 93-574, 5 USC 522a)
13. Department of Commerce, *Report of the working Group on Department-wide Information Technology Security Program, Recommended ITS Program Structure*, September 28, 2001.

## **Appendix III**

### **Working Group Members**

Carl Boykin, Health and Human Services

Paulette Dawson, OCIO/Commerce

Herschel Gelman, NTIA/Commerce

JeanAnn Guyette, OCIO/Commerce

Pat Heinig, BXA/Commerce

Linda Laboskie, NOAA/Commerce

Tim Ruland, Census/Commerce

Eric Williams, Technical Advisor

## **Appendix IV**

### **Modified FISCAM**

## APPENDIX IV

### Modified FISCAM

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
AC-1 Classify information resources according to their criticality and sensitivity.				
AC-1.1 Resource classifications and related criteria have been established.	Classifications and criteria have been established and communicated to resource owners.	Review policies and procedures.  Interview resource owners.		
AC-1.2 Owners have classified resources.	Resources are classified based on risk assessments; classifications are documented and approved by an appropriate senior official and are periodically reviewed.	Review resource classification documentation and compare to risk assessments. Discuss any discrepancies with appropriate officials.		
AC-2 Maintain a current list of authorized users and their access authorized.				
AC-2.1 Resource owners have identified authorized users and their access authorized.	Access authorizations are documented on standard forms and maintained on file, approved by senior managers, and securely transferred to security managers.	Review pertinent written policies and procedures.  For a selection of users (both application user and IS personnel) review access authorization documentation.		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
	Owners periodically review access authorization listings and determine whether they remain appropriate.	Interview owners and review supporting documentation. Determine whether inappropriate access is removed in a timely manner.		
	The number of users who can dial into the system from remote locations is limited and justification for such access is documented and approved by owners. (See section AC-3.2 for additional controls over dial-up access.)	For a selection of users with dial-up access, review authorization and justification.		
	Security managers review access authorizations and discuss any questionable authorizations with resource owners.	Interview security managers and review documentation provided to them.		
AC-2.1 Resource owners have identified authorized users and their access authorized. (continued)	All changes to security profiles by security managers are automatically logged and periodically reviewed by management independent of the security function. Unusual activity is investigated.	Review a selection of recent profile changes and activity logs.		
	Security is notified immediately when system users are terminated or transferred.	Obtain a list of recently terminated employees from Personnel and, for a selection, determine whether system access was promptly terminated.		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
AC-2.2 Emergency and temporary access authorization is controlled.	Emergency and temporary access authorizations are documented on standard forms and maintained on file, approved by appropriate managers, securely communicated to the security function; and automatically terminated after a predetermined period.	Review pertinent policies and procedures.  Compare a selection of both expired and active temporary and emergency authorizations (obtained from the authorizing parties) with a system-generated list of authorized users.  Determine the appropriateness of access documentation and approvals and the timeliness of terminating access authorization when no longer needed.		
AC-2.3 Owners determine disposition and sharing of data.	Standard forms are used to document approval for archiving, deleting, or sharing data files.	Examine standard approval forms.  Interview data owners.		
	Prior to sharing data or programs with other entities, agreements are documented regarding how those files are to be protected.	Examine documents authorizing file sharing and file sharing agreements.		
AC-3 Establish physical and logical				

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
controls to prevent or detect unauthorized access.				
AC-3.1 Adequate physical security controls have been implemented.		<i>These audit procedures should be coordinated with section SC-2.2 (environmental controls) since many of the control objectives and techniques are the same.</i>		
A. Physical safeguards have been established that are commensurate with the risks of physical damage or access.	<p>Facilities housing sensitive and critical resources have been identified.</p> <p>All significant threats to the physical well-being of sensitive and critical resources have been identified and related risks determined.</p>	<p>Review a diagram of the physical layout of the computer, telecommunications, and cooling system facilities.</p> <p>Walk through facilities.</p> <p>Review risk analysis.</p>		
	<p>Access is limited to those individuals who routinely need access through the use of guards, identification badges, or entry devices, such as key cards.</p> <p>Management regularly reviews the list of persons with physical access to sensitive facilities.</p>	<p>Review lists of individuals authorized access to sensitive areas and determine the appropriateness for access.</p> <p>Before becoming recognized as the auditor, attempt to access sensitive areas</p>		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
		<p>without escort or identification badges.</p> <p>Observe entries to and exits from facilities during and after normal business hours.</p> <p>Observe utilities access paths.</p> <p>Interview management.</p>		
	Keys or other access are needed to enter the computer room and tape/media library.	<p>Observe entries to and exits from sensitive areas during and after normal business hours.</p> <p>Interview employees.</p>		
A. Physical safeguards have been established that are commensurate with the risks of physical damage or access. (continued)	All deposits and withdrawals of tapes and other storage media from the library are authorized and logged.	<p>Review procedures for the removal and return of storage media from and to the library.</p> <p>Select from the log some returns and withdrawals, verify the physical existence of the tape or other media, and determine whether proper authorization was</p>		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
		obtained for the movement.		
	Unissued keys or other entry devices are secured.	Observe practices for safeguarding keys and other devices.		
	Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to reenter after fire drills, etc.	Review written emergency procedures.  Examine documentation supporting prior fire drills.  Observe a fire drill.		
B. Visitors are controlled.	Visitors to sensitive areas, such as the main computer room and tape/media library, are formally signed in and escorted.	Review visitor entry logs.  Observe entries to and exits from sensitive areas during and after normal business hours.  Interview guards at facility entry.		
	Entry codes are changed periodically.	Review documentation on and logs of entry code changes.		
	Visitors, contractors, and maintenance personnel are authenticated through the use of	Observe appointment and verification procedures for visitors.		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
	preplanned appointments and identification checks.			
AC-3.2 Adequate logical access controls have been implemented.				
A. Passwords, tokens, or other devices are used to identify and authenticate users.	<p>Passwords are unique for specific individuals, not groups; controlled by the assigned user and not subject to disclosure; changed periodically--every 30 to 90 days;</p> <p>not displayed when entered; at least 6 alphanumeric characters in length; and prohibited from reuse for at least 6 generations.</p>	<p>Review pertinent policies and procedures.</p> <p>Interview users.</p> <p>Review security software password parameters.</p> <p>Observe users keying in passwords.</p> <p>Attempt to log on without a valid password; make repeated attempts to guess passwords.</p> <p>Assess procedures for generating and communicating passwords to users.</p>		
	Use of names or words is prohibited.	Review a system-generated list of current passwords.		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
		Search password file using audit software.		
	Vendor-supplied passwords are replaced immediately.	Attempt to log on using common vendor supplied passwords.  Search password file using audit software.		
	Generic user IDs and passwords are not used.	Interview users and security managers.  Review a list of IDs and passwords.		
	Attempts to log on with invalid passwords are limited to 3-4 attempts.	Repeatedly attempt to log on using invalid passwords.  Review security logs.		
A. Passwords, tokens, or other devices are used to identify and authenticate users.(continued)	Personnel files are automatically matched with actual system users to remove terminated or transferred employees from the system.	Review pertinent policies and procedures.  Review documentation of such comparisons.  Interview security managers.		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
		Make comparison using audit software.		
	Password files are encrypted.	View dump of password files (e.g., hexadecimal printout).		
	For other devices, such as tokens or key cards, users maintain possession of their individual tokens, cards, etc, and understand that they must not loan or share these with others and must report lost items immediately.	Interview users  To evaluate biometric or other technically sophisticated authentication techniques, the auditor should obtain the assistance of a specialist.		
B. Identification of access paths.	An analysis of the logical access paths is performed whenever system changes are made.	Review access path diagram.		
C. Logical controls over data files and software programs.	Security software is used to restrict access.  Access to security software is restricted to security administrators only.	Interview security administrators and system users.  Review security software parameters.		
	Computer terminals are automatically logged off after a period of inactivity.	Observe terminals in use.  Review security software		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
		parameters.		
	Inactive users' accounts are monitored and removed when not needed.	<p>Review security software parameters.</p> <p>Review a system-generated list of inactive logon IDs, and determine why access for these users has not been terminated.</p>		
C. Logical controls over data files and software programs. (continued)	<p>Security administration personnel set parameters of security software to provide access as authorized and restrict access that has not been authorized. This includes access to data files, load libraries, batch operational procedures, source code libraries, security files, and operating system files.</p> <p>Naming conventions are used for resources.</p>	<p>Determine library names for sensitive or critical files and libraries and obtain security reports of related access rules. Using these reports, determine who has access to critical files and libraries and whether the access matches the level and type of access authorized.</p> <p>Perform penetration testing by attempting to access and browse computer resources including critical data files, production load libraries, batch operational procedures (e.g., JCL libraries), source code libraries, security</p>		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
		<p>software, and the operating system. These tests should be performed as (1) an "outsider" with no information about the entity's computer systems; and (2) an "outsider" with prior knowledge about the systems--e.g., an ex-insider, and (3) an "insider" with and without specific information about the entity's computer systems, and with access to the entity's facilities.</p> <p>When performing outsider tests, test the controls over external access to computer resources, including networks, dial-up, LAN, WAN, RJE, and the Internet.</p> <p>When performing insider tests, use an ID with no special privileges to attempt to gain access to computer resources beyond those available to the account. Also, try to access the</p>		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
		entity's computer resources using default/generic IDs with easily guessed passwords.  Determine whether naming conventions are used.		
D. Logical controls over a database.	Database management systems (DBMS) and data dictionary (DD) controls have been implemented that restrict access to data files at the logical data view, field, or field-value level; control access to the DD using security profiles and passwords; maintain audit trails that allow monitoring of changes to the DD; and provide inquiry and update capabilities from application program functions, interfacing DBMS or DD facilities	Review pertinent policies and procedures.  Interview database administrator.  Review DBMS and DD security parameters.  Test controls by attempting access to restricted files.		
	Use of DBMS utilities is limited.	Review security system parameters.		
	Access and changes to DBMS software are controlled.			
	Access to security profiles in the DD and security tables in the DBMS is limited.			

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
E. Logical controls over telecommunications access.	<p>Communication software has been implemented to verify terminal identifications in order to restrict access through specific terminals; verify IDs and passwords for access to specific applications; control access through connections between systems and terminals; restrict an application's use of network facilities; protect sensitive data during transmission; automatically disconnect at the end of a session; maintain network activity logs; restrict access to tables that define network options, resources, and operator profiles; allow only authorized users to shut down network components; monitor dial-in access by monitoring the source of calls or by disconnecting and then dialing back at preauthorized phone numbers; restrict in-house access to telecommunications software; control changes to telecommunications software; ensure that data are not accessed or modified by an unauthorized</p>	<p>Review pertinent policies and procedures.</p> <p>Review parameters set by communications software or teleprocessing monitors.</p> <p>Test telecommunications controls by attempting to access various files through communications networks.</p> <p>Identify all dial-up lines through automatic dialer software routines and compare with known dial-up access. Discuss discrepancies with management.</p> <p>Interview telecommunications management staff and users.</p>		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
	user during transmission or while in temporary storage; and restrict and monitor access to telecommunications hardware or facilities.			
	<p>In addition to logical controls:</p> <p>The opening screen viewed by a user provides a warning and states that the system is for authorized use only and that activity will be monitored.</p> <p>Dial-in phone numbers are not published and are periodically changed.</p>	<p>Review pertinent policies and procedures.</p> <p>View the opening screen seen by telecommunication system users.</p> <p>Review documentation showing changes to dial-in numbers.</p> <p>Review entity's telephone directory to verify that the numbers are not listed.</p>		
AC-3.3 Cryptographic tools.	Cryptographic tools have been implemented to protect the integrity and confidentiality of sensitive and critical data and software programs.	To evaluate cryptographic tools, the auditor should obtain the assistance of a specialist.		
AC-3.4 Sanitation of equipment and media prior to disposal or reuse.	Procedures are implemented to clear sensitive data and software from discarded and transferred equipment and media.	<p>Review written procedures.</p> <p>Interview personnel responsible for clearing</p>		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
		<p>equipment and media.</p> <p>For a selection of recently discarded or transferred items, examine documentation related to clearing of data and software.</p> <p>For selected items still in the entity's possession, test that they have been appropriately sanitized.</p>		
AC-4 Monitor access, investigate apparent security violations, and take appropriate remedial action.				
AC-4.1 Audit trails are maintained.	All activity involving access to and modifications of sensitive or critical files is logged.	Review security software settings to identify types of activity logged.		
AC-4.2 Actual or attempted unauthorized, unusual, or sensitive access is monitored.	Security violations and activities, including failed logon attempts, other failed access attempts, and sensitive activity, are reported to management and investigated.	<p>Review pertinent policies and procedures.</p> <p>Review security violation reports.</p> <p>Examine documentation showing reviews of questionable activities.</p>		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
AC-4.3 Suspicious access activity is investigated and appropriate action taken.	Security managers investigate security violations and report results to appropriate supervisory and management personnel.  Appropriate disciplinary actions are taken.	Test a selection of security violations to verify that follow-up investigations were performed and to determine what action were taken against the perpetrator.		
	Violations are summarized and reported to senior management.	Interview senior management and personnel responsible for summarizing violations.  Review any supporting documentation.		
	Access control policies and techniques are modified when violations and related risk assessments indicate that such changes are appropriate.	Review policies and procedures and interview appropriate personnel.  Review any supporting documentation.		
CC-1 Processing features and program modifications are properly authorized.				
CC-1.1 A system development life cycle methodology (SDLC) has been implemented.	A SDLC methodology has been developed that provides a structured approach consistent with generally accepted concepts and practices, including active user involvement throughout the process, is	Review SDLC methodology.  Review system documentation to verify that SDLC methodology was followed.		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
	sufficiently documented to provide guidance to staff with varying levels of skill and experience, provides a means of controlling changes in requirements that occur over the system's life, and includes documentation requirements.			
	Program staff and staff involved in developing and testing software have been trained and are familiar with the use of the organization's SDLC methodology	Interview staff.  Review training records.		
CC-1.2 Authorizations for software modifications are documented and maintained.	Software change request forms are used to document requests and related approvals.  Change requests must be approved by both system users and data processing staff.	Identify recent software modifications and determine whether change request forms were used.  Examine a selection of software change request forms for approvals.  Interview software development staff.		
CC-1.3 Use of public domain and personal software is restricted.	Clear policies restricting the use of personal and public domain software have been developed and are enforced.  The entity uses virus identification	Review pertinent policies and procedures  Interview users and data processing staff.		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
	software.			
CC-2 Test and approve all new and revised software.				
CC-2.1 Changes are controlled as programs progress through testing to final approval.	Test plan standards have been developed for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, library control).	Review test plan standards.		
	Detailed system specifications are prepared by the programmer and reviewed by a programming supervisor.	For the software change requests selected for control activity CC-1.2: review specifications; trace changes from code to design specifications; review test plans; compare test documentation with related test plans; analyze test failures to determine if they indicate ineffective software testing; review test transactions and data;		
	Software changes are documented so that they can be traced from authorization to the final approved code and they facilitate "trace-back" of code to design specifications and functional requirements by system testers.			

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
	Test plans are documented and approved that define responsibilities for each party involved (e.g., users, systems analysts, programmers, auditors, quality assurance, library control).			
	Unit, integration, and system testing are performed and approved <ul style="list-style-type: none"> <li>· in accordance with the test plan and</li> <li>· applying a sufficient range of valid and invalid conditions.</li> </ul>			
	A comprehensive set of test transactions and data is developed that represents the various activities and conditions that will be encountered in processing.  Live data are not used in testing of program changes, except to build test data files.			
CC-2.1 Changes are controlled as programs progress through testing to final approval. (continued)	Test results are reviewed and documented.	For the software change requests selected for control activity CC-1.2 (continued): review test results; review documentation of management or security administrator reviews; verify user acceptance; and		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
		<p>review updated documentation.</p> <p>Determine whether operational systems experience a high number of abend and, if so, whether they indicate inadequate testing prior to implementation.</p>		
	Program changes are moved into production only upon documented approval from users and system development management.			
	Documentation is updated for software, hardware, operating personnel, and system users when a new or modified system is implemented.			
	Data center management and/or the security administrators periodically review production program changes to determine whether access controls and change controls have been followed.			
CC-2.2 Emergency changes are promptly tested and approved.	Emergency change procedures are documented.	Review procedures.		
	Emergency changes are documented	For a selection of emergency		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
	and approved by the operations supervisor, · formally reported to computer operations management for follow-up, and · approved after the fact by programming supervisors and user management.	changes recorded in the emergency change log, review related documentation and approval.		
CC-2.3 Distribution and implementation of new or revised software is controlled.	Standardized procedures are used to distribute new software for implementation.	Examine procedures for distributing new software.		
	Implementation orders, including effective date, are provided to all locations where they are maintained on file.	Examine implementation orders for a sample of changes.		
CC-3 Control software libraries.				
CC-3.1 Programs are labeled and inventoried.	Library management software is used to produce audit trails of program changes, · maintain program version numbers, · record and report program changes, · maintain creation/date information for production modules,	Review pertinent policies and procedures.  Interview personnel responsible for library control.  Examine a selection of programs maintained in the		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
	<ul style="list-style-type: none"> <li>maintain copies of previous versions, and control concurrent updates.</li> </ul>	<p>library and assess compliance with prescribed procedures.</p> <p>Determine how many prior versions of software modules are maintained.</p>		
CC-3.2 Access to program libraries is restricted.	Separate libraries are maintained for program development and maintenance, testing, and production programs.	<p>Examine libraries in use.</p> <p>Interview library control personnel.</p>		
	Source code is maintained in a separate library.	<p>Examine libraries in use.</p> <p>Verify that source code exists for a selection of production load modules by (1) comparing compile dates, (2) recompiling the source modules, and (3) comparing the resulting module size to production load modules size.</p>		
	Access to all programs, including production code, source code, and extra program copies, are protected by access control software and operating system features.	For critical software production programs, determine whether access control software rules are clearly defined.		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
		Test access to program libraries by examining security system parameters.		
	All deposits and withdrawals of program tapes to/from the tape library are authorized and logged.	Select some program tapes from the log and verify the existence of the tapes either in the library or with the individual responsible for withdrawing the tapes.		
SS-1 Limit access to system software.				
SS-1.1 Access authorizations are appropriately limited.	Policies and procedures for restricting access to systems software exist and are up-to-date.	<p>Review pertinent policies and procedures.</p> <p>Interview management and systems personnel regarding access restrictions.</p> <p>Observe personnel accessing system software, such as sensitive utilities, and note the controls encountered to gain access.</p> <p>Attempt to access the</p>		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
		operating system and other system software.		
	Access to system software is restricted to a limited number of personnel, corresponding to job responsibilities. Application programmers and computer operators are specifically prohibited from accessing system software.			
	Documentation showing justification and management approval for access to system software is kept on file.	<p>Select some systems programmers and determine whether management-approved documentation supports their access to system software.</p> <p>Select some application programmers and determine whether they are not authorized access.</p>		
	The access capabilities of system programmers are periodically reviewed for propriety to see that access permissions correspond with job duties.	Determine the last time the access capabilities of system programmers were reviewed.		
SS-1.2 All access paths have been identified and controls	The operating system is configured to prevent circumvention of the	Test the operating system parameters to verify that it		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
implemented to prevent or detect access for all paths.	security software and application controls.	is configured to maintain the integrity of the security software and application controls. (The specifics of this step will be determined by the operating system in use. The auditor should consult audit guides for the operating system in use. This step may be facilitated by use of CA-EXAMINE, the DEC VAX Toolkit, or other audit tools. However, the auditor should be experienced in using the specific software tool, or seek the assistance of someone who is.)		
		Obtain a list of vendor-supplied software and determine if any of these products have known deficiencies that adversely impact the operating system integrity controls.  Judgmental review of the installation of system software components and		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
		determine whether they were appropriately installed to preclude adversely impacting operating system integrity controls.		
SS-1.2 All access paths have been identified and controls implemented to prevent or detect access for all paths. (continued)	The operating system is configured to prevent circumvention of the security software and application controls. (continued)	<p>Perform an operating system penetration analysis to determine if users can inappropriately utilize computer resources through direct or covert methods including:</p> <p>Determine whether the operating system's subsystems have been appropriately implemented to ensure that they support integrity controls. (For example, with MVS, the auditor should evaluate IPL controls; APF update controls and implementation of key MVS libraries and locally defined and tailored system libraries; SVC controls, including imbedded passwords and controls to</p>		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
		<p>prevent interception; SMF options; and PPT.)</p> <p>Determine whether applications interfaces have been implemented to support operating system integrity controls, including on-line transaction monitors; database software; on-line editors; on-line direct-access storage devices; on-line operating system datasets; exits related to the operating system, security, and program products; and controls over batch processing, to include security controls, scheduler controls, and access authorities. (For example, with MVS, the evaluated interfaces should include CICS, ADABAS, IMS, IDMS, TSO and/or similar packages; on-line DASD volumes; and on-line MVS datasets, such as CLIST, PARMLIB, SPOOL,</p>		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
		DUMP, and TRACE, I/O appendages, and JES2/JES3.)		
SS-1.2 All access paths have been identified and controls implemented to prevent or detect access for all paths. (continued)	The operating system is configured to prevent circumvention of the security software and application controls. (continued)	<p>Perform an operating system penetration analysis to determine if users can inappropriately utilize computer resources through direct or covert methods including: (continued)</p> <p>Evaluate the controls over external access to computer resources including networks, dial-up, LAN, WAN, RJE, and the Internet.</p> <p>Identify potential opportunities to adversely impact the operating system and its products through Trojan horses, viruses, and other malicious actions.</p>		
	Access to system software is restricted to personnel with corresponding job responsibilities	Obtain a list of all system software on test and production libraries used by		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
	by access control software. Update access should generally be limited to primary and backup systems programmers. All accesses to system software files are logged by automated logging facilities.	<p>the entity.</p> <p>Verify that access control software restricts access to system software.</p> <p>Using security software reports, determine who has access to system software files, security software, and logging files. Preferably, reports should be generated by the auditor, but at a minimum, they should be generated in the presence of the auditor.</p> <p>Verify that system programmer's access to production data and programs is only allowed under controlled updates and during emergencies when established procedures are followed.</p>		
SS-1.2 All access paths have been identified and controls implemented to prevent or detect access for all paths. (continued)	Vendor-supplied default logon IDs and passwords have been disabled.	<p>Inquire whether disabling has occurred.</p> <p>Test for default presence</p>		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
		using vendor standard IDs and passwords.		
	Remote access to the system master console is restricted. Physical and logical controls provide security over all terminals that are set up as master consoles.	<p>Determine what terminals are set up as master consoles and what controls exist over them.</p> <p>Test to determine if the master console can be accessed or if other terminals can be used to mimic the master console and take control of the system.</p>		
SS-2 Monitor access to and use of system software.				
SS-2.1 Policies and techniques have been implemented for using and monitoring use of system utilities.	Policies and procedures for using and monitoring use of system software utilities exist and are up-to-date.	<p>Review pertinent policies and procedures.</p> <p>Interview management and systems personnel regarding their responsibilities.</p>		
	Responsibilities for using sensitive system utilities have been clearly defined and are understood by systems programmers.			

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
	Responsibilities for monitoring use are defined and understood by technical management.			
	The use of sensitive system utilities is logged using access control software reports or job accounting data (e.g., IBM's System Management Facility).	Determine whether logging occurs and what information is logged.  Review logs.  Using security software reports, determine who can access the logging files.		
SS-2.2 Inappropriate or unusual activity is investigated and appropriate actions taken.	The use of privileged system software and utilities is reviewed by technical management.	Interview technical management regarding their reviews of privileged system software and utilities usage.  Review documentation supporting their reviews.		
	Inappropriate or unusual activity in using utilities is investigated.	Interview management and systems personnel regarding these investigations.  Review documentation supporting these		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
		investigations.		
SS-3 Control system software changes.				
SS-3.1 System software changes are authorized, tested, and approved before implementation.	Policies and procedures exist and are up-to-date for identifying, selecting, installing, and modifying system software. Procedures include an analysis of costs and benefits and consideration of the impact on processing reliability and security.	Review pertinent policies and procedures.  Interview management and systems personnel.		
	Procedures exist for identifying and documenting system software problems. This should include using a log to record the problem, the name of the individual assigned to analyze the problem, and how the problem was resolved.	Review procedures for identifying and documenting system software problems.  Interview management and systems programmers.  Review the causes and frequency of any recurring system software problems, as recorded in the problem log, and ascertain if the change control process should have prevented these problems.		
SS-3.1 System software changes	New system software versions or	Determine what		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
are authorized, tested, and approved before implementation. (continued)	products and modifications to existing system software receive proper authorization and are supported by a change request document.	<p>authorizations and documentation are required prior to initiating system software changes.</p> <p>Select recent system software changes and determine whether the authorization was obtained and the change is supported by a change request document.</p>		
	<p>New system software versions or products and modifications to existing system software are tested and the test results are approved before implementation. Procedures include:</p> <ul style="list-style-type: none"> <li>· a written standard that guides the testing, which is conducted in a test rather than production environment;</li> <li>· specification of the optional security-related features to be turned on, when appropriate;</li> <li>· review of test results by technically qualified staff who document their opinion on whether the system software is ready for</li> </ul>	<p>Determine the procedures used to test and approve system software prior to its implementation.</p> <p>Select recent system software changes and test whether the indicated procedures were in fact used.</p>		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
	<ul style="list-style-type: none"> <li>production use; and</li> <li>· review of test results and documented opinions by data center management prior to granting approval to move the system software into production use.</li> </ul>			
	<p>Procedures exist for controlling emergency changes. Procedures include:</p> <ul style="list-style-type: none"> <li>· authorizing and documenting emergency changes as they occur;</li> <li>· reporting the changes for management review; and</li> </ul> <p>review by an independent IS supervisor of the change.</p>	<p>Review procedures used to control and approve emergency changes.</p> <p>Select some emergency changes to system software and test whether the indicated procedures were in fact used.</p>		
SS-3.2 Installation of system software is documented and reviewed.	Installation of system software is scheduled to minimize the impact on data processing and advance notice is given to system users.	<p>Interview management and systems programmers about scheduling and giving advance notices when system software is installed.</p> <p>Review recent installations and determine whether scheduling and advance notification did occur.</p>		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
		Determine whether better scheduling and notification of installations appears warranted to reduce impact on data processing operations.		
	<p>Migration of tested and approved system software to production use is performed by an independent library control group.</p> <p>Outdated versions of system software are removed from production libraries.</p>	<p>Interview management, systems programmers, and library control personnel, and determine who migrates approved system software to production libraries and whether outdated versions are removed from production libraries.</p> <p>Review supporting documentation for some system software migrations and the removal of outdated versions from production libraries.</p>		
	Installation of all system software is logged to establish an audit trail and reviewed by data center management.	Interview data center management about their role in reviewing system software installations.		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
		Review some recent system software installations and determine whether documentation shows that logging and management review occurred.		
SS-3.2 Installation of system software is documented and reviewed. (continued)	Vendor-supplied system software is still supported by the vendor.	Interview system software personnel concerning a selection of system software and determine the extent to which the operating version of the system software is currently supported by the vendor.		
	All system software is current and has current and complete documentation.	Interview management and systems programmers about the currency of system software and the currency and completeness of software documentation.  Review documentation and test whether recent changes are incorporated.		
SD-1 Segregate incompatible duties and establish related policies.				
SD-1.1 Incompatible duties have	Policies and procedures for	Review pertinent policies		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
been identified and policies implemented to segregate these duties.	segregating duties exist and are up-to-date.	and procedures.  Interview selected management and IS personnel regarding segregation of duties.		
	<p>Distinct systems support functions are performed by different individuals, including the following:</p> <ul style="list-style-type: none"> <li>• IS management.</li> <li>• System design.</li> <li>• Application programming.</li> <li>• Systems programming.</li> <li>• Quality assurance/testing.</li> <li>• Library management/change management.</li> <li>• Computer operations.</li> <li>• Production control and scheduling.</li> <li>• Data control.</li> <li>• Data security.</li> <li>• Data administration.</li> <li>• Network Administration.</li> </ul>	<p>Review an agency organization chart showing IS functions and assigned personnel.</p> <p>Interview selected personnel and determine whether functions are appropriately segregated.</p> <p>Determine whether the chart is current and each function is staffed by different individuals.</p> <p>Review relevant alternate or backup assignments and determine whether the proper segregation of duties is maintained.</p> <p>Observe activities of</p>		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
		personnel to determine the nature and extent of the compliance with the intended segregation of duties.		
SD-1.1 Incompatible duties have been identified and policies implemented to segregate these duties. (continued)	<p>No individual has complete control over incompatible transaction processing functions. Specifically, the following combination of functions are not performed by a single individual:</p> <ul style="list-style-type: none"> <li>· Data entry and verification of data.</li> <li>· Data entry and its reconciliation to output.</li> <li>· Input of transactions for incompatible processing functions (e.g., input of vendor invoices and purchasing and receiving information).</li> <li>· Data entry and supervisory authorization functions (e.g., authorizing a rejected transaction to continue processing that exceeds some limit requiring a supervisor's</li> </ul>	<p>Review the organizational chart and interview personnel to determine that assignments do not result in a single person being responsible for the indicated combinations of functions.</p> <p>Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.</p>		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
	review and approval).			
	Organizations with limited resources to segregate duties have compensating controls, such as supervisory review of transactions performed.	Interview management, observe activities, and test transactions. <i>Note: Perform this in conjunction with SD-3.2.</i>		
	Data processing personnel are not users of information systems. They and security managers do not initiate, input, or correct transactions .	Determine through interview and observation whether data processing personnel and security managers are prohibited from these activities.		
	Day-to-day operating procedures for the data center are adequately documented and prohibited actions are identified.	Review the adequacy of documented operating procedures for the data center.		
	Regularly scheduled vacations and periodic job/shift rotations are required (see SP-4.1 on personnel policies).	<i>Audit procedures are found in section SP-4.1, but this item is listed here as a reminder. Individuals performing incompatible duties and acting inappropriately could be detected when another individual undertakes those duties. Requiring vacations and rotations helps detect</i>		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
		<i>such actions.</i>		
SD-1.2 Job descriptions have been documented.	Documented job descriptions accurately reflect assigned duties and responsibilities and segregation of duty principles.	<p>Review job descriptions for several positions in organizational units and for user security administrators.</p> <p>Determine whether duties are clearly described and prohibited activities are addressed.</p> <p>Review the effective dates of the position descriptions and determine whether they are current.</p> <p>Compare these descriptions with the current responsibilities and duties of the incumbents in these positions to determine the accuracy of these statements.</p>		
	Documented job descriptions include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position and can be used for hiring, promoting, and	Review job descriptions and interview management personnel.		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
	performance evaluation purposes.			
SD-1.3 Employees understand their duties and responsibilities.	All employees fully understand their duties and responsibilities and carry out those responsibilities in accordance to their job descriptions.	Interview personnel filling positions for the selected job descriptions (see above). Determine if the descriptions match their understanding of their duties and responsibilities and whether additional duties are undertaken that are not listed in their job descriptions.		
	Senior management is responsible for providing adequate resources and training to ensure that segregation of duty principles are understood and established, enforced, and institutionalized within the organization.	Determine from interviewed personnel whether senior management has provided adequate resources and training to establish, enforce, and institutionalize the principles of segregation of duties.		
	Responsibilities for restricting access by job positions in key operating and programming activities are clearly defined, understood, and followed.	Interview management personnel in these activities.		
SD-2 Establish access controls to enforce segregation of duties.				
SD-2.1 Physical and logical access controls have been established.	Physical and logical access controls help restrict employees to authorized actions based upon organizational	Interview management and subordinate personnel. <i>Note: This audit step should</i>		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
	and individual job responsibilities.	<i>be performed in conjunction with audit steps in section AC-3.</i>		
SD-2.2 Management reviews effectiveness of control techniques.	Staff's performance should be monitored on a periodic basis and controlled to ensure that objectives laid out in job descriptions are carried out.	Interview management and subordinate personnel.  Select documents or actions requiring supervisory review and approval for evidence of such performance (e.g., approval of input of transactions, software changes).		
	Management reviews are performed to determine that control techniques for segregating incompatible duties are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (e.g., periodic risk assessments).	Determine which reviews are conducted to assess the adequacy of duty segregation. Obtain and review results of such reviews. <i>Note: This audit step should be performed in conjunction with audit steps in critical elements SP-1 and SP-5.</i>		
SD-3 Control personnel activities through formal operating procedures and supervision and review.				
SD-3.1 Formal procedures guide	Detailed, written instructions exist	Review manuals.		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
personnel in performing their duties.	and are followed for the performance of work.	Interview supervisors and personnel.  Observe processing activities.		
	Operator instruction manuals provide guidance on system operation.			
	Application run manuals provide instruction on operating specific applications.			
	Operators are prevented from overriding file label or equipment error messages.			
SD-3.2 Active supervision and review are provided for all personnel.	Personnel are provided adequate supervision and review, including each shift for computer operations.	Interview supervisors and personnel  Observe processing activities.  Review history log reports for signatures indicating supervisory review.  Determine who is authorized to perform the initial		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
		program load for the system, what steps are followed, and what controls are in place to monitor console activity during the process. Determine whether operators override the IPL parameters.		
	All operator activities on the computer system are recorded on an automated history log.			
	Supervisors routinely review the history log and investigate any abnormalities.			
	System startup is monitored and performed by authorized personnel. Parameters set during the initial program load (IPL) are in accordance with established procedures.			
SC-1 Assess the criticality and sensitivity of computerized operations and identify supporting resources.				
SC-1.1 Critical data and operations are identified and prioritized.	A list of critical operations and data has been documented that <ul style="list-style-type: none"> <li>· prioritizes data and operations,</li> <li>· is approved by senior program managers, and</li> </ul>	Review related policies.  Review list and any related documentation.		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
	reflects current conditions.	Interview program, data processing, and security administration officials. Determine their input and their assessment of the reasonableness of priorities established.		
SC-1.2 Resources supporting critical operations are identified.	Resources supporting critical operations have been identified and documented. Types of resources identified should include <ul style="list-style-type: none"> <li>· computer hardware,</li> <li>· computer software,</li> <li>· computer supplies,</li> <li>· system documentation,</li> <li>· telecommunications,</li> <li>· office facilities and supplies, and</li> <li>· human resources.</li> </ul>	Review related documentation.  Interview program and security administration officials.		
SC-1.3 Emergency processing priorities are established.	Emergency processing priorities have been documented and approved by appropriate program and data processing managers.	Review related policies.  Review related documentation.  Interview program and security administration officials.		
SC-2 Take steps to prevent and				

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
minimize potential damage and interruption.				
SC-2.1 Data and program backup procedures have been implemented.	Backup files are created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are lost or damaged.	<p>Review written policies and procedures for backing up files.</p> <p>Compare inventory records with the files maintained off-site and determine the age of these files.</p> <p>For a selection of critical files, locate and examine the backup files. Verify that backup files can be used to recreate current reports.</p> <p>Determine whether backup files are created and rotated off-site as prescribed and are sent before prior versions are returned.</p>		
	System and application documentation are maintained at the off-site storage location.	Locate and examine documentation.		
	The backup storage site is geographically removed from the primary site(s), and	Examine the backup storage site.		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
	protected by environmental controls and physical access controls.			
SC-2.2 Adequate environmental controls have been implemented.		<i>These procedures should be performed in conjunction with Section AC-3.3, regarding physical access controls.</i>		
	<p>Fire suppression and prevention devices have been installed and are working, e.g., smoke detectors, fire extinguishers, and sprinkler systems.</p> <p>Controls have been implemented to mitigate other disasters, such as floods, earthquakes, etc.</p> <p>Redundancy exists in the air cooling system.</p> <p>Building plumbing lines do not endanger the computer facility or, at a minimum, shut-off valves and procedures exist and are known.</p> <p>An uninterruptible power supply or backup generator has been provided so that power will be adequate for</p>	<p>Examine the entity's facilities.</p> <p>Interview site managers.</p> <p>Observe that operations staff are aware of the locations of fire alarms, fire extinguishers, regular and auxiliary electrical power switches, water shut-off valves, breathing apparatus, and other devices that they may be expected to use in an emergency.</p> <p>Observe the operation, location, maintenance and access to the air cooling systems.</p>		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
	orderly shut down.	<p>Observe whether water can enter through the computer room ceiling or pipes are running through the facility and that there are water detectors on the floor.</p> <p>Determine whether the activation of heat and smoke detectors will notify the fire department.</p>		
	Environmental controls are periodically tested.	<p>Review test policies.</p> <p>Review documentation supporting recent tests of environmental controls.</p>		
	Eating, drinking, and other behavior that may damage computer equipment is prohibited.	<p>Review policies and procedures regarding employee behavior.</p> <p>Observe employee behavior.</p>		
SC-2.3 Staff have been trained to respond to emergencies.	All data center employees have received training and understand their emergency roles and responsibilities.	<p>Interview data center staff.</p> <p>Review training records</p>		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
	<p>Data center staff receive periodic training in emergency fire, water, and alarm incident procedures.</p> <p>Emergency response procedures are documented.</p>	<p>Review training course documentation.</p> <p>Review emergency response procedures.</p>		
	<p>Emergency procedures are periodically tested.</p>	<p>Review test policies.</p> <p>Review test documentation.</p> <p>Interview data center staff.</p>		
SC-2.4 Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions.	<p>Policies and procedures exist and are up-to-date.</p>	<p>Review policies and procedures.</p>		
	<p>Routine periodic hardware preventive maintenance is scheduled and performed in accordance with vendor specifications and in a manner that minimizes the impact on operations.</p>	<p>Interview data processing and user management.</p> <p>Review maintenance documentation.</p>		
	<p>Regular and unscheduled maintenance performed is documented.</p>			
	<p>Flexibility exists in the data</p>			

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
	processing operations to accommodate regular and a reasonable amount of unscheduled maintenance.			
	Spare or backup hardware is used to provide a high level of system availability for critical and sensitive applications.	Interview data center management.		
	Goals are established by senior management on the availability of data processing and on-line services.	Interview senior management, data processing management, and user management.  Review supporting documentation.		
	Records are maintained on the actual performance in meeting service schedules.			
SC-2.4 Effective hardware maintenance, problem management, and change management help prevent unexpected interruptions. (continued)	Problems and delays encountered, the reason, and the elapsed time for resolution are recorded and analyzed to identify recurring patterns or trends.	Interview senior management, data processing management, and user management.  Review supporting documentation.		
	Senior management periodically reviews and compares the service			

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
	performance achieved with the goals and surveys user departments to see if their needs are being met.			
	Changes of hardware equipment and related software are scheduled to minimize the impact on operations and users, thus allowing for adequate testing.			
	Advance notification on hardware changes is given to users so that service is not unexpectedly interrupted.			
SC-3 Develop and document a comprehensive contingency plan.				
SC-3.1 An up-to-date contingency plan is documented.	<p>A contingency plan has been documented that</p> <ul style="list-style-type: none"> <li>· reflects current conditions,</li> <li>· has been approved by key affected groups including senior management, data center management, and program managers,</li> <li>· clearly assigns responsibilities for recovery,</li> <li>· includes detailed instructions for restoring operations (both operating system and critical applications),</li> <li>· identifies the alternate processing facility and the backup storage facility,</li> </ul>	<p>Review the contingency plan and compare its provisions with the most recent risk assessment and with a current description of automated operations.</p> <p>Interview senior management, data center management, and program managers.</p>		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
	<ul style="list-style-type: none"> <li>· includes procedures to follow when the data/service center is unable to receive or transmit data,</li> <li>· identifies critical data files,</li> <li>· is detailed enough to be understood by all agency managers,</li> <li>· includes computer and telecommunications hardware compatible with the agencies needs, and</li> <li>· has been distributed to all appropriate personnel.</li> </ul>			
	<p>The plan provides for backup personnel so that it can be implemented independent of specific individuals.</p> <p>User departments have developed adequate manual/peripheral processing procedures for use until operations are restored.</p>	<p>Review the contingency plan.</p> <p>Interview senior management, data center management, and program managers.</p>		
SC-3.1 An up-to-date contingency plan is documented. (continued)	Several copies of the current contingency plan are securely stored off-site at different locations.	Observe copies of the contingency plan held off-site.		
	The contingency plan is periodically reassessed and, if appropriate, revised to reflect changes in hardware, software, and personnel	Review the plan and any documentation supporting recent plan reassessments.		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SC-3.2 Arrangements have been made for alternate data processing and telecommunications facilities.	<p>Contracts or interagency agreements have been established for a backup data center and other needed facilities that</p> <ul style="list-style-type: none"> <li>· are in a state of readiness commensurate with the risks of interrupted operations,</li> <li>· have sufficient processing capacity, and</li> <li>· are likely to be available for use.</li> </ul> <p>Alternate telecommunication services have been arranged.</p> <p>Arrangements are planned for travel and lodging of necessary personnel, if needed.</p>	Review contracts and agreements.		
SC-4 Periodically test the contingency plan and adjust it as appropriate.				
SC-4.1 The plan is periodically tested.	The current plan has been tested under conditions that simulate a disaster.	<p>Review policies on testing.</p> <p>Review test results.</p> <p>Observe a disaster recovery test.</p>		

Control Activities	Control Techniques	Audit Procedures	Work Paper References	Assessment of Control Effectiveness
SC-4.2 Test results are analyzed and contingency plans are adjusted accordingly.	Test results were documented and a report, such as a "lessons learned" report, was developed and provided to senior management.	Review final test report.  Interview senior managers to determine if they are aware of the test results.		
	The contingency plan and related agreements and preparations were adjusted to correct any deficiencies identified during testing.	Review any documentation supporting contingency plan adjustments.		